

# Certificate implementation— The good, the bad, and the ugly

---

*DOE ER/DP Security R&D Workshop*

James A. Rome

Oak Ridge National Laboratory

March 19, 1998

# A wealth of riches?

---

I decided to use certificates for strong authentication, but which ones?

- Entrust
- Entrust WebCA
- Netscape
- SSLeay
- Microsoft IIS

Issues are:

Cost, compatibility, ease of use, flexibility, security

# Issues to consider

---

- Do the CA's issue the certificates or do the customers apply for them?
- What is the role of a directory server? Is it integrated into the CA?
- Can certificates (easily) be used for non-Web applications?
- Can the DN contain the information you need?
- Will the certificates work in MS & Netscape browsers? Apache, Netscape, MS, ... servers?

# Generated-secret method

---

- CA creates a certificate request file ("bulk add file") containing the names and certificate types of the users.
- The CA software returns a list of reference numbers and authorization codes. These "generated secrets" uniquely identify each user.
- You must distribute them securely to each user. Each user then visits the Client Interface and enters this information to retrieve the certificate. This generates the keys.

# Existing-secret method

---

- Use if the CA doesn't know the names and locations of the people who need certificates, or you don't have a secure way of transmitting reference number and authorization code.
- Users generate key pair *before* the request and put the public key in the certificate request.
- Must verify the user's identity. In some cases this can be done using an "existing secret" such as a PIN.
- Certificate is only useful for private key holder.

# Certificate server comparison

	Entrust	WebCA	Netscape	SSLeay
<b>\$/Cert</b>	\$140 \$33/year	\$1	free, \$121 \$5+\$10+25	free
<b>Ease of customization</b>	Done in LDAP	Configura- tion file	Easy	
<b>CA Queryable?</b>	No	with difficulty	yes	
<b>SDK?</b>	Yes (\$5k)	No	Yes (free)	No
<b>Initiation</b>	CA	User/CA	User	CA
<b>LDAP integration</b>	Yes	Built-in, queries=?	Manual	No

# Prices are hard to figure lately . . .

Product	Base Offering (Includes Media and License)		Price for 10 Additional Users License-Only Pack
	\$ Price	No. of User Licenses	
SuiteSpot Standard Edition	\$5600	50	\$600
Calendar Server	\$1750	50	\$350
Collabra Server	\$525	50	\$100
Directory Server	\$995	100	\$100
Enterprise Pro Server	\$1995	50 (Netshare users)	not applicable
Enterprise Server	\$1295	50 (Netshare users)	\$250 (10 Netshare users)
Messaging Server	\$1295	50	\$250
SuiteSpot Professional Edition	\$7000	50	\$1,025
Certificate Server	\$525	100	\$50
Compass Server	\$1295	50	\$250
Mission Control Desktop	\$995	50	\$200
Proxy Server	\$525	100	\$50
FastTrack Server	\$295	not applicable	not applicable

# And there is lots of gamemanship

## NETSCAPE SUITESPOT VERSUS MICROSOFT EXCHANGE AND BACKOFFICE

Price per User Comparison of Shrink-Wrap Product Offerings\*

Product	50 Users	100 Users	250 Users	500 Users	1000 Users
BackOffice with SQL Server Internet Connector	329.48	263.93	233.06	230.94	230.94
BackOffice	269.50	233.94	221.06	218.95	218.95
BackOffice Small Business Server with SQL Server Internet Connector	140.06	100.93	77.45		
Exchange Enterprise Edition with SQL Server and SQL Server Internet Connector	303.46	244.25	201.41	210.66	214.38
Exchange Standard Edition with SQL Server and SQL Server Internet Connector	275.44	230.24	195.81	202.76	205.33
SuiteSpot Professional Edition	140.00	121.24	109.98	106.23	104.36
Exchange Enterprise Edition**	101.34	81.03	66.23	69.26	70.46
SuiteSpot Standard Edition	82.00	71.00	64.40	62.20	61.10
Exchange Standard Edition**	73.32	67.02	60.62	61.36	61.40



# Browsers and certificates

---

- How do they handle multiple certificates?
  - ▶ 1 certificate/e-mail address.
- No interchange mechanism between IE and Netscape. MS says “yes” but it doesn’t work.
  - ▶ Turns out it is a known “unadvertised” registry misentry. IE4 128-bit upgrade install fails to update registry to use 128-bit for all operations.
- Can certificates be spoofed? — Yes
  - ▶ NS accepts every certificate in signed E-mail and overwrites existing certificate entry.

# CA issues

---

- No obvious “accept CA” mechanism
  - ▶ Certificate is invalid if the CA not on your “approved” list. But no info on how to get the CA certificate.
- Most certificates do not contain CRL URL.
- In IE it is very difficult (maybe impossible) to import a Netscape CA root certificate. Netscape exports it in base-64 format. IE requires DER.
- In IE 3, it was impossible to form an https SSL session because the site certificate’s CA was not accepted. Hence impossible to get to the CA.

# CA unknown failure

**These are certificates from other people**

allendb1@ornl.gov

elgamal@netscape.com

jimgeuin@cyberservices.com

lpz@ornl.gov

lspitz@newlogic.com

mgmlyna@iname.com

**wej@george.lbl.gov**


wejohnston@lbl.gov

wrightmc@ornl.gov

yannig@fiu.edu

To get certificates from a network Directory


Search Directory

 **View A Personal Certificate - Netscape**

**This Certificate belongs to:**  
William E. Johnston  
wej@george.lbl.gov  
ICSD  
Lawrence Berkeley National Laboratory  
US

**This Certificate was issued by:**  
IDCG-CA  
ICSD  
Lawrence Berkeley National Laboratory  
US

**Serial Number:** 2E  
**This Certificate is valid from** Fri Feb 06, 1998 **to** Sat Jul 31, 1999  
**Certificate Fingerprint:**  
46:93:D1:F6:4B:C1:F5:68:02:EA:AF:A3:E8:D7:F2:77

 **Verify A Certificate - Netscape**

Verification of the selected certificate failed for the following reasons:

**wej@george.lbl.gov**  
Unable to find Certificate Authority

# Web servers and certificates

---

- By default what does a server do with a client certificate? Is it checked for
  - ▶ validity?
  - ▶ Revocation? (Even Verisign has no CRL)
  - ▶ the CA validity?
  - ▶ anything??
- The certificate does not contain information about the certificate server or the LDAP server that stores the associated user information. So, where do you access them?

# Client authentication

---

- A client (such as a browser) requests a connection with the server.
- The server is authenticated or not (through the process of server authentication).
- The client signs but does not encrypt its certificate and sends it to the server.
- The server uses the client's public key, which is included in the certificate, to verify that the owner of the certificate is the same one who signed it.

# Client authentication (cont.)

---

- The server attempts to match the certificate authority to a trusted certificate authority. If the client's certificate is not listed as trusted, the transaction ends, and the client receives: "The server cannot verify your certificate."
- If the client's certificate authority is trusted, some servers fulfill the transaction. (!!)
- The server only accepts the desired client CAs. This is good if you want to restrict access to users with your certificates only.

# Client authentication (cont.)

---

- Next, the server needs to match the information from the certificate with an entry in an LDAP directory to further identify and authenticate the user. If all information matches, the server accepts the client as authenticated.
- If entries in your database contain certificates rather than information, the server compares the sent certificate to the one in the database. If they match, the server grants the client access.

# How to use DN without LDAP

---

*Netscape says:*

“Use the Access-Control API to implement your own attribute getter function for the user attribute when the authentication method is SSL. Your attribute getter function can extract the issuer and subject DNs from the user certificate and construct SQL queries to the third-party database.”

*Microsoft says:*

“It is all in the platform development kit”  
Its easier said than done....